The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
9/14/2010

SUBJECT:
Vulnerability in Print Spooler Could Allow Remote Code Execution (MS10-061)

OVERVIEW:
A vulnerability has been identified in the Microsoft Print Spooler service. The Print Spooler service is used for local and remote printing and is enabled on Windows systems by default. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Microsoft has reported that the vulnerability is being actively exploited at this time.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been identified in Microsoft Print Spooler service that could allow an attacker to take complete control of an affected system. The Print Spooler service is used for managing local and remote printing and is enabled on Windows systems by default.

The vulnerability is caused by the Microsoft Print Spooler service incorrectly restricting user permissions to access print spoolers. An attacker can exploit this vulnerability by sending a specially crafted print request to a system which has an exposed print spooler interface over Remote Procedure Call (RPC). Affected systems running Windows XP are most vulnerable as they allow guest access to shared print services. On all other vulnerable versions of Windows, an attacker will be required to authenticate to the server unless they have been configured to allow anonymous access.

Successful exploitation of these vulnerabilities could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Microsoft has reported that the vulnerability is being actively exploited at this time.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Disable Printer Sharing unless there is a business need to do otherwise.
- Block ports associated with RPC at the network boundary unless there is a documented business need.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-061.mspx

Security Focus:
http://www.securityfocus.com/bid/43073

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2729

Secunia:
http://secunia.com/advisories/41292